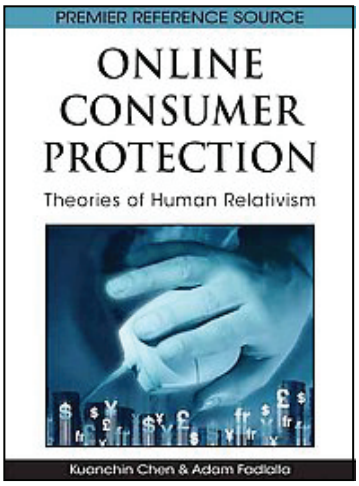
BOOK REVIEW

ONLINE CONSUMER PROTECTION. THEORIES OF HUMAN RELATIVISM

Sofia Elena Colesca *
The Bucharest Academy of Economic Studies, Romania

Kuanchin Chen and Adam Fadlalla
Online consumer protection. Theories of Human Relativism



We are living in a world where information collection, explore and exchange is done more and more easily using the Internet. Each user should be aware that the Internet is a two-way connection: the user first connects to the Internet to gather information, but, on the other hand, any web resource can collect information about users, their computer site, location, operating system, browsing habits or other information that may be the user would like to keep it confidential. The nature of these online threats is often unclear to the average of Internet users. Where do these threats originate? Who wants to invade our privacy? What kind of information do they want, and what do they want to do with it? How could be protected against online threats? In order to answer to these questions *"Online Consumer Protection: Theories of Human Relativism"* presents to the academic community a collections of informational essays dealing with issues related to privacy and data protection when using electronic sources of communication and data transfer, put together by Professor *Kuanchin Chen* of Western Michigan University and Professor *Adam Fadlalla* of Cleveland State University.

The book is structured in 19 chapters grouped into five sections: *Background* (chapters I-III), *Frameworks and Models* (chapters IV-VII), *Empirical Assessments* (chapters VIII-X), *Consumer Privacy in Business* (chapters XI-XIV), and *Policies, Techniques and Laws for Protection* (chapters XV-XIX).

It is said that the best security is provided by a system that has no access. Unfortunately, such as system would hardly be usable by anyone. There has always been a trade-off between accessibility and security, and usability and privacy. With an increasing online presence, individual and corporate users need to reevaluate the security and privacy angle. In this respect, the *background section* provides an overview of online privacy.

* Author's contact: e-mail: sofiac@man.ase.ro

Search engines are very important tools on the Internet today and Google is the leader in this field. It is appreciated for its simple interface and fast services offered at no evident cost. On the other hand, many people worry of Google's increasing power as the ultimate arbiter of commercial success ("to exist is equal to be indexed by the search engine") and as a central database for users' personal information, e-mails, calendars, photos, videos, blogs, documents, social networks, news feeds – in short, their entire digital lives. Google's access to and storage of vast amounts of personal data create a serious privacy problem, so, in *chapter I - „Google: Technological Convenience vs. Technological Intrusion"*, Pauxtis and White are investigating the privacy implications of online search, giving an overview of Google's services and how they are related to privacy online. The conclusion was that the vast majority of Internet users either do not know Google's data collection policies, or simply do not care about them.

In *chapter II – „A Taxonomic View of Consumer Online Privacy Legal Issues, Legislation and Litigation"* are discussed the consumer online privacy legal issues. Secor and Tarn present the major research studies focusing on information security breaches, information privacy breaches, identity theft and pre-texting, health information privacy, underage consumer protection, and spyware, malware, viruses, cookies and SPAM. A relational model is presented to explore the relation between online privacy legislation, litigation, legal protection, remedies and risks for not complying with the legal requirements.

As the number of businesses and customers transaction over the Internet is increasing, threats and risks accompanying them also increase. In order to protect the organization from variuos types of attacks, management need to understand what they are fighting against. As response to these questions, *chapter III - "Online Privacy, Vulnerabilities and Threats: A Manager's Perspective"*, provides a management perspective on the issues confronting managers which conduct business in an online environment. Sockel and Falk present an overview of the various vulnerabilities, threats, and actions that are commonly used and may be sufficient for many Web-based transactions, to prevent attacks and to protect the privacy of an organization, its customers, and its employees.

The second section *"Frameworks and Models",* composed of four chapters, presents some frameworks and models for analysis of privacy issues.

In Chapter IV –"*Practical Privacy Assessments",* Jansen, Peen and Jensen are presenting the Operational Privacy Assessment Model, based on an evaluation of all the organizational, operational and technical factors that are relevant to the protection of personal data stored and managed in an computerized systems. The different factors are measured on a simple scale and the results presented in a simple graphical form, which makes it easy to compare two systems to each other or to identify the factors that benefit most from improved privacy enhancing technologies.

Trust is one of the most formidable barriers for people engaging in online relationships. Trust in online transactions has some unique features because the impersonal nature of the online environment, the extensive use of technology, and the inherent uncertainty and risk of using an open infrastructure. Privacy concerns has a great influence on trust. Individuals want to be able to release personal information in the confident belief that it will only be used in the way the individual intended. Providing this assurance is the key to demonstrating trustworthiness. According with this idea, in chapter V – *"Privacy and Trust in Online Interactions"*, Lilien and Bhargava are presenting different trust models, the close

relationship between trust and privacy in online environments and the metrics for these two related concepts.

Despite privacy protection legislation, guidelines, and codes of practice are available, their effectiveness is limited in alleviating consumers' privacy and security concerns, so, in chapter VI - *"Current Measures To Protect E-Consumers' Privacy In Australia",* Ha, Coghill, and Maharaj present the Australian's experience in privacy protection.

Many studies have shown that privacy concerns act as obstacles in the use of online transactions. In a synthesis of the research in the field of online privacy, in Chapter VII - *"Antecedents of Online Privacy Protection Behavior: Towards an Integrated Model",* Gurung and Jain identified the existing frameworks and variables related to online privacy. The analysis showed how the privacy construct is used with other related constructs from different perspective. Since only one study specifically examined the privacy protection behavior, the authors felt the need to understand the privacy concerns of consumers and consequent strategies taken by consumers to protect their online privacy. As result they have developed an integrative framework of online privacy protection behavior.

The third section "*Empirical Assessments*", presents some empirical findings on various privacy subjects. A first study is presented by Rea and Chen in chapter VIII – "*Privacy Control and Assurance: Does Gender Influence Online Information Exchange?*" who explored the relationships between gender, trust, concern and consumers' online privacy. The results showed that there is a significant difference in gender tendencies and privacy concerns, but other factors such Internet experience, culture, learning styles, age, education should be counted in evaluation of the impact over the privacy concerns. The findings should be useful for IT managers in the development of their privacy policies.

The next study, presented in Chapter IX – "*A Profile of the Demographics, Psychological Predispositions, and Social/Behavioral Patterns of Computer Hacker Insiders and Outsiders*", analyses the psychological and behavioral composition of hackers and the social dynamics that they operate within. The authors of this study, Schell and Holt, argue that the understanding of these behavioral patterns can help in the development of effective techniques and best practices to limit the hackers' activities.

Despite high concerns of some consumers about privacy in online transaction, they still disclose sensitive personal information. In order to explain this dilemma, in the last chapter of section 3,"*Privacy Or Performance Matters On The Internet: Revisiting Privacy Toward A Situational Paradigm"* (chapter X), Hsu examines the privacy concerns within two contexts: technology platforms and users' motivation. The results showed that consumers' privacy concerns do not reflect their privacy practices and showed how social contexts influence consumers' privacy practices.

The fourth section is composed of four chapters focused on consumer privacy in business.

The advent of digital media and analog/digital conversion technologies brings an extraordinary increase in the amount of information that can be easily and inexpensively reproduced. Given the widespread availability of computers, many people now have the ability to casually reproduce vast amounts of information. Consequently, the traditional physical and economic impediments to copyright infringement have been considerably undermined. The concerns are higher for copyright-dependent individuals and organizations, especially within the music and movie industries, because these individuals

and organizations are partly or wholly dependent on the revenue generated from such works. As a response to these types of challenges, Chan, Collins, and Movafaghi explore in chapter XI - *"Online Consumer Privacy and Digital Rights Management Systems"*, different Digital Rights Management (DRM) strategies. DRM is a generic term to describe any technology that inhibits uses of digital content that were not desired or foreseen by the content provider.

Advertising dominates every sphere of our life. And Internet is not an exception. Much of our online experience is being shaped to better serve advertisers. A fast growing segment of Internet advertising is behavioral advertising, which requires tracking consumers as they perform personal searches and interact with various web sites. Information gathered from tracking is used by online advertising networks to develop consumer profiles used for more targeted advertising. In respect with this, in chapter XII – *"Online Privacy and Marketing: Current Issues for Consumers and Marketers"*, Parker analyses the online privacy concerns from a marketing perspective. The discussed subjects include the use of spy ware and cookies, word-of-mouth marketing, online marketing to children and the use of social networks.

The most of Internet sites collect at least one type of personal information (name, e-mail address or postal address). Although Internet users are generally dissatisfied with the way data is gathered over the Internet, they would provide information if given assurance that they are not identified. Disclose of information usage policies could encourage users to provide information and conduct transactions online. To test this assumption, in chapter XIII – *"An Analysis of Online Privacy Policies of Fortune 100 Companies",* Li and Zhang present the result of a survey on Fortune 100 Companies in respect with online privacy policy. The conclusion of this study is that "a well designed privacy policy by itself is not adequate to guarantee privacy protection, effective implementation is as important. Consumer education and awareness are also essential for privacy protection".

Different people, cultures, and nations have a wide variety of expectations about online privacy. In chapter 14 – "*Cross Cultural Perceptions On Privacy In The United States, Vietnam, Indonesia And Taiwan"*, Chiou, Chen, and Bisset examine some social and cultural differences between the mentioned countries in respect with online privacy. The results of a survey conducted by the authors showed that "collectivistic cultures appear to be less sensitive to the violation of personal privacy; while the individualistic cultures are found to be more proactive in privacy protection".

Today, personal information about an individual is being collected at a rate and to a degree unthinkable even five years ago. Currently, much of an individual's personal information can be legally collected, shared, exchanged, sold, and disseminated without notice to or input by the individual. Online privacy can be protected or regulated online by the market, norms, laws or codes. Drawing on the American, European and Japanese experiences, the fifth section "*Policies, Techniques and Laws For Protection*" explores the complex interdependence among online privacy, law, technology and industry practices.

In chapter XV – *"Biometric Controls and Privacy",* Lancaster and Yen provide a descriptive discussion of the current state of biometrics. Biometrics use some unique human characteristics (fingerprint, iris, voice, hand geometry, face and signature) to identify a user. Discussion is focused in four main areas, technological soundness, economic values, business applications and legal/ethical concerns.

In the last decade, governments around the world have been working to capture the vast potential of information and communication technologies to improve government processes. Increasing use of information technologies in government processes has raised issues about the privacy of information provided by citizens and business to government. Confidential business information and private personal information may be vulnerable when data are in government hands. Thus, in chapter XVI - *"Government Stewardship of Online Information: FOIL Requirements and Other Considerations"* Erickson analyses the contradictions between openness of government and personal privacy.

While the Internet has become the dominant environment for delivery and exchange of information, the regulation of this media has never reached an international common ground. Nations, due to their legal perspectives and cultural differences, tend to regulate the Internet in their own way. In respect with this, the last three chapters "*The Legal Framework for Data and Consumer Protection in Europe*", "*Cybermedicine, Telemedicine and Data Protection in the United States*" and "*Online Privacy Protection in Japan: The Current Status and Practices*", present the legal framework and the law of the European Union, United States and Japan in the field of online consumer protection, with the emphasis putting on trans-border differences in the concepts of privacy. The insight provided in this chapters could help policy makers of the leading nations in the cyberspace to improve their mutual understanding in the quest for establishing a global legal environment for the Internet.

As a conclusion, I would recommend the book as a useful acquisition for any researcher, department and library serving social science and computer science.

About the authors

Ph. D. Kuanchin Chen is Associate Professor of Computer Information Systems at the Department of Business Information Systems, Western Michigan University, where he teaches courses in electronic business, web architecture, portals, systems development, and business analysis.

Dr. Chen fields of research are: e-business, e-commerce, online privacy, trust and security, online behavioral issues, Internet addiction and dependency, online media use, web services and data mining. His research work was rewarded with several awards ranging from best paper to research scholar. He received the 2008-2009 Emerging Scholar Award.

Dr. Chen has published numerous articles in journals and other academic publication outlets. Some representative works are:

- The acceptance and diffusion of the innovative smart phone use: A case study of a delivery service company in logistics, Information and Management, 46(4): 241:248
- An exploratory study of the selection of communication media: The relationship between flow and communication outcomes. *Decision Support Systems* 45(4): 822-832
- Capturing industry experience for an effective information security assessment. *IJISCM* 1(4): 421-438

- Distance learning, virtual classrooms, and teaching pedagogy in the Internet environment, *Technology in Society*, 26(4): 585-598

Ph. D. Adam Fadlalla is a Professor of Computer and Information Science at the College of Business Administration, Cleveland State University. His research interests covers a broad spectrum of information systems issues: decision support systems, artificial intelligence applications, knowledge discovery in databases, information systems security and privacy issues, enterprise integration systems, and medical informatics.

Trained in both Economics and Computers, Dr. Fadlalla holds a B.S. in Business Administration from the University of Khartoum, an M.B.A. in Finance from the Miami University, and M.S. and Ph.D in Computer Science from University of Cincinnati. He received the prestigious Fulbright Scholarship, in 2004 and 2005.

His research has been published in many journals, including *Computers and Operations Research, Omega, Interfaces, Journal of the American Medical Informatics, Association and Information Systems Management*. Some representative works of Dr. Fadlalla are

- Constraint isomorphism and the generation of stochastic data. *IIE Transactions*, Taylor & Francis Ltd, 38(5): 437-444.
- A Framework for Assessing E-Health Preparedness, *International Journal of Electronic Healthcare*, 1(3): 316-334
- An experimental investigation of the impact of aggregation on the performance of data mining with logistic regression, *Information & Management*, 42(5): 695-707
- Data Warehouse Administration and Management, *IS Management*, 17(1): 1-10